(19) BUNDESREPUBLIK DEUTSCHLAND

—DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 197 05 620 A 1**

(51) Int. Cl.[6]:
G 07 C 9/00
G 07 F 7/12
G 06 K 19/073
H 04 L 9/32
H 04 L 12/22

(21) Aktenzeichen: 197 05 620.2
(22) Anmeldetag: 14. 2. 97
(43) Offenlegungstag: 3. 9. 98

DE 197 05 620 A 1

(71) Anmelder:
ESD Information Technology Entwicklungs GmbH, 04430 Dölzig, DE

(74) Vertreter:
Haußingen, P., Ing. Faching. f. Schutzrechtswesen, Pat.-Anw., 06526 Sangerhausen

(72) Erfinder:
Bugovics, Jozsef, 06886 Lutherstadt Wittenberg, DE

(56) Entgegenhaltungen:

DE	43 17 380 C1
DE	43 06 819 C2
DE	37 04 814 C2
DE	195 48 903 A1
DE	195 07 043 A1
DE	44 06 602 A1
DE	44 06 601 A1
DE	43 08 825 A1
DE	41 38 861 A1
DE	39 27 270 A1
DE	39 04 215 A1
EP	05 52 392 B1
EP	07 27 894 A1
EP	05 32 102 A2

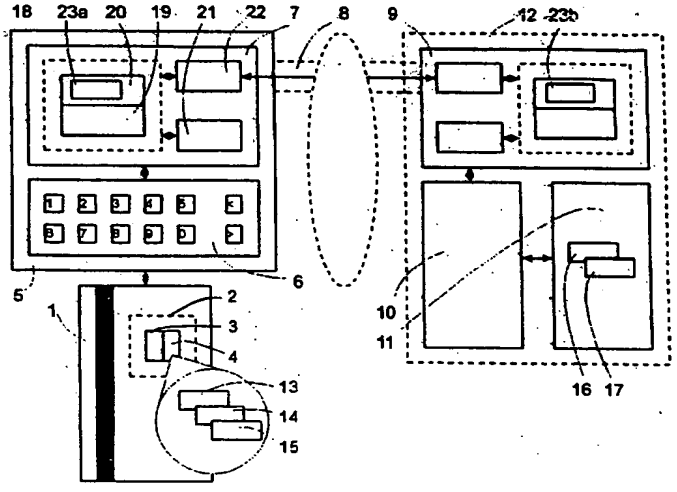
BEUTELSPACHER A., et al.: Chipkarten als Sicherheitswerkzeug, Berlin, Springer, 1991, Kap.2, S. 5-13;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Anordnung und Verfahren zur dezentralen Chipkartenidentifikation

(57) Die Erfindung bezeichnet eine Anordnung und ein Verfahren zur dezentralen Chipkartenidentifikation, deren Aufgabe darin besteht, die Identifizierung einer Chipkarte (1) und die Prüfung des berechtigten Zugangs eines Benutzers derart vorzunehmen, daß diese bei vergleichbarer Sicherheit ohne das vor Ort notwendige zweite Rechenwerk in geschützter Umgebung und damit kostengünstiger möglich wird.
Ein wesentliches Merkmal der Erfindung besteht darin, daß das notwendige zweite Rechenwerk in geschützter Umgebung nicht vor Ort, sondern an zentraler Stelle als zentrales Rechenwerk (10) betrieben wird. Durch eine in der Erfindung beschriebene Lösung wird zur Kommunikation ein sicherer Kanal (8) zwischen einem speziellen Terminal (6), welches keine geheimen Informationen der Art beinhaltet, das sie in einer geschützten Umgebung gekapselt werden müssen, und damit wesentlich kostengünstiger produzierbar und breit verfügbar wird, und dem zentralen Rechenwerk (10) mit zu schützenden geheimen Informationen an zentraler Stelle in einer geschützten Umgebung (12), aufgebaut.



DE 197 05 620 A 1

Beschreibung

Die Erfindung bezeichnet eine Anordnung und ein Verfahren zur dezentralen Chipkartenidentifikation, welches vor Ort ohne die verschlüsselnde Einheit in geschützter Umgebung auskommt.

Chipkarten werden durch die Integration von Mikrocontrollern in Plastikkarten gekennzeichnet. Im Unterschied zu Karten, die lediglich ein Speichermedium bereitstellen bsw. einen Magnetstreifen oder einen Halbleiterspeicher, sind diese Chipkarten bei anliegender Versorgungsspannung als selbständige Rechenwerke tätig, die Programme abarbeiten. Bekanntestes Beispiel für eine derartige Chipkarte ist die. Smartcard. Durch die Kombination von Speichereinheit und Rechenwerk auf einer checkkartengroßen Plastikkarte, die meist noch mit weiteren Informationen bsw. Schriftzeichen, Fotos, Hologrammen versehen ist, ist der Einsatz der Chipkarte als Identifikationsmittel oder Speichermedium sehr vielfältig.

Ein Einsatzgebiet der Chipkarte wird durch die Verwendung im bargeldlosen Zahlungsverkehr bestimmt. Für die damit verbunden Sicherheitsanforderungen ist es notwendig, eine zur Identifizierung der Chipkarte und damit ihres berechtigten Benutzers dienende PIN (persönliche Identifizierungsnummer) auf der Karte geeignet sicher und unmanipulierbar abzulegen. Für die Benutzung der Karte im Sinne ihrer Verwendung wird diese PIN bsw. über ein Eingabeterminal eingegeben und über den Mikrocontroller auf der Karte, welcher seine Versorgungsspannung aus dem Terminal bezieht, auf ihre Gültigkeit hin zu vergleichen. Handelt es sich um eine gültige PIN, wird die aufgerufene Applikation, bsw das Bedienungsprogramm zum Zugriff auf die Konten einer Bank, für den Benutzer freigeschalten. Im gegenteiligen Fall wird meist eine Routine zur Fehlerbehandlung aufgerufen, durch welche die Möglichkeit, die gültige PIN durch wiederholtes Probieren zu ermitteln, ausgeschlossen wird.

Die früher im bargeldlosen Zahlungsverkehr verwendeten Karten enthielten als Speichermedium einen Magnetstreifen, der mit relativ einfachen Mitteln ausgelesen werden konnte. Durch ein derartiges Auslesen der auf der Karte gespeicherten PIN, wäre der berechtigte Zugang für unberechtigte Dritte zu leicht zu erkunden. Zur Gewährleistung der notwendig hohen Sicherheit im bargeldlosen Zahlungsverkehr war es nicht ausreichend, eine PIN direkt auf der Karte abzulegen und diese mit der über das Terminal eingegebenen PIN zu vergleichen. Aus diesem Grund wird die PIN, mit Zusatzinformationen aus der Kartenidentifikationsdatei versehen, in verschlüsselter Weise auf der Karte als EPIN (Encipher PIN) hinterlegt. Zur Verschlüsselung dienen hauptsächlich Algorithmen des DES (Data Encryption Standard) oder auf diesem basierende Modifikationen bsw. Triple-DES (dreimalige Anwendung des DES). Aufgrund der mit der Koexistenz von Karten mit Magnetstreifen und Chipkarten verbundenen Kompatibilitätsprobleme im Übergangszeitraum werden in vielen Fällen die Chipkarten für den bargeldlosen Zahlungsverkehr zusätzlich mit einem Magnetstreifen versehen. Die Information der PIN wird in der gleichen Art im Chip wie im Magnetstreifen, also als EPIN, gespeichert. Mit Hilfe dieser Verschlüsselungsalgorithmen und eines Schlüssel, welcher aus einer vielstelligen Zahl gebildet wird, besteht die Möglichkeit, die codierte Information zu entschlüsseln und anschließend auf ihre Gültigkeit hin zu überprüfen. Dieser Vorgang ist prinzipiell mittels des Mikrocontrollers der Chipkarte durchführbar. Es ergibt sich jedoch das Problem, daß durch Dritte mit hinreichender krimineller Energie das Programm der Chipkarte sowie der abgespeicherte Schlüssel ausgelesen werden können. Mit deren Kenntnis bestände dann die Möglichkeit, diese Chipkarte und insbesondere alle weiteren Chipkarten bzw. die sie repräsentierenden Konten zu manipulieren. Um dieses Problem zu umgehen, sind die Algorithmen und der zugehörige Schlüssel nicht auf der Chipkarte, sondern in einer hinreichend geschützten Umgebung auf einem zweiten Rechenwerk hinterlegt. Zur Überprüfung der gültigen Nutzungsberechtigung wird die über das Termin eingegebene PIN dem zweiten Rechenwerk, welches sich in der geschützten Umgebung befindet, bsw. in einem gepanzerten Behälter am Bankautomaten der ec-Karte, übergeben, dort mit den geheimen Algorithmen und Schlüsseln verschlüsselt und schließlich mit der codiert abgespeicherten EPIN der Chipkarte verglichen. Mit diesem Verfahren ist eine hinreichende Sicherheit für den bargeldlosen Zahlungsverkehr gewährleistet, da weder die geheimen Algorithmen noch die Schlüssel einem Dritten zugänglich sind. Allerdings hat diese Sicherheit ihren Preis. Die Kosten für das zweite Rechenwerk in der geschützten Umgebung belaufen sich auf ca. DM 2100,–. Dabei versuchen die Schutzmechanismen gegen unbefügtes Öffnen der geschützten Umgebung den wesentlichen Anteil dieser Kosten. Derartig aufwendige Systeme sind bei dieser Lösung an jedem Endterminal notwendig, wodurch aus Kosten- und Sicherheitsgründen die Anzahl der Systeme, bsw. der Bankautomaten, auf einige wenige Standorte begrenzt bleibt.

Der Erfindung liegt die Aufgabe zugrunde, eine Anordnung und ein Verfahren zur dezentralen Chipkartenidentifikation zu entwickeln, welche es gestattet, die Identifizierung einer Chipkarte und die Prüfung des berechtigten Zugangs eines Benutzers derart vorzunehmen, daß diese bei vergleichbarer Sicherheit ohne das vor Ort notwendige zweite Rechenwerk in geschützter Umgebung und damit kostengünstiger möglich wird. Damit soll die Voraussetzung zur Nutzung von Chipkarten bei Anwendungen mit hohen Sicherheitsanforderungen von zahlreichen und kostengünstigen Datenterminals aus möglich werden.

Die Aufgabe der Erfindung wird durch die in den Patentansprüchen 1 und 2 bezeichneten Merkmale gelöst. Bevorzugte Weiterbildungen ergeben sich aus den Unteransprüchen. Ein wesentliches Merkmal der Erfindung besteht darin, daß das notwendige zweite Rechenwerk in geschützter Umgebung nicht vor Ort, sondern an zentraler Stelle betrieben wird. Durch eine in der Erfindung beschriebene Lösung wird ein sicherer Kommunikationskanal zwischen einem speziellen Terminal, welches keine geheimen Informationen der Art beinhaltet, das sie in einer geschützte Umgebung gekapselt werden müssen, und damit wesentlich kostengünstiger produzierbar und breit verfügbar wird, und dem zweiten Rechenwerk mit zu schützenden geheimen Informationen an zentraler Stelle, aufgebaut.

Die Anordnung wird anschließend an Hand von **Fig. 1** näher erläutert.

Eine Chipkarte **1** mit einem Mikrocontroller **2**, der ein integriertes Rechenwerk **3** und einen integrierten Speicher **4** beinhaltet, befindet sich zur verwendungsgemäßen Benutzung in einem speziellen Chipkartenleser **5**, der ein Terminal **6** und ein Kommunikationsmodul I **7** beinhaltet, welches über einen sicheren Kanal **8** mit einem Kommunikationsmodul II **9** in Wirkverbindung steht, wobei das Kommunikationsmodul II **9** mit einem zentralen Rechenwerk **10** und einem zentralen Speicher **11** verbunden ist, welche sich in einer geschützten Umgebung **12** befinden. Die Chipkarte **1** bezieht die für ihren Betrieb notwendige Versorgungsspannung über den speziellen Chipkartenleser **5**. Im integrierten Speicher **4** der Chipkarte **1** ist eine kartenindividuelle verschlüsselte EPIN **13** und ein ebenfalls kartenindividueller Schlüssel K_{PIN} **14** sowie weitere kartenindividuelle und in

bestimmten Mengen einheitliche Schlüssel K_{sonst} 15 abgelegt, die mittels geeigneter Generierungsschlüssel an zentraler Stelle dynamisch generiert werden. Die Generierung der kartenindividuellen Schlüssel erfolgt mittels Kartenidentifikationsdaten CID (Card Identification Data) und Generierungsschlüsseln KGK (Key Generating Key). In dem zentralen Speicher 11 des zentralen Rechenwerks 10 befindet sich innerhalb der geschützten Umgebung 12 ein für alle Chipkarten einheitlicher Schlüssel K_{PS} 16 und ein ebenfalls für alle Chipkarten einheitlicher Schlüssel KGK_{PIN} 17, welche von der ZKA (zentrale Kreditanstalt) herausgegeben werden.

Die funktionell ähnlichen Kommunikationsmodule I, II 7, 9 bestehen jeweils aus einem Kommunikationsmikrocontroller 18, in dem eine interne CPU 19, ein interner Speicher 20, ein Selektionsmodul 21 und ein Interface 22 angeordnet sind. Die Funktionsweise dieser Kommunikationsmodule I, II 7, 9 ist derart, daß jedes Kommunikationsmodul I, II 7, 9 mittels des Selektionsmoduls 21 eindeutig identifizierbar ist, wobei mittels jeweils an autorisierter Stelle speziell generierten Schlüssel K_{Komm} 23, die durch Dritte nicht auslesbar sind, mittels Verschlüsselung der sichere Kanal 8 zwischen je zwei derartigen Kommunikationsmodule I, II 7, 9 aufgebaut werden kann. Das Interface 22 bezeichnet eine Schnittstelleneinheit zu einer geeigneten Zugangsstelle eines Datennetzes bsw. eine serielle Schnittstelle zum Anschluß an einen PC (Personal Computer), welcher einen Zugang zum Internet besitzt. Im Interesse eines hohen Datendurchsatzes kann das Kommunikationsmodul II 9 entsprechend rechenleistungsgemäß, bsw. mittels Parallelbetrieb, ausgelegt sein.

Das Verfahren zur dezentralen Chipkartenidentifikation verläuft in nachfolgenden Schritten.

In einem ersten Schritt initialisiert der Benutzer durch die Inbetriebnahme des Chipkartenlesers 5 und durch das Einführen der Chipkarte 1 in den Chipkartenleser 5 die einzelnen verwendeten Module, wobei in allen aktiven Mikrocontrollern die entsprechenden Grundinitialisierungsroutinen abgearbeitet werden.

In einem zweiten Schritt gibt der Benutzer zur Bezeichnung seiner Zugriffsberechtigung für die durch die Chipkarte 1 sicherheitsgemäß geschützte Anwendung über das Terminal 6 seine PIN ein und bestätigt die korrekte Eingabe.

In einem dritten Schritt baut das Kommunikationsmodul I 7 des Chipkartenlesers 5 einen sicheren Kanal 8 mit dem Kommunikationsmodul II 9 des zentralen Rechenwerkes 10 innerhalb der geschützten Umgebung 12 auf. Dies geschieht durch Verschlüsselung der zu übermittelnden Daten mit Hilfe des Schlüssels K_{Komm} 23. Da dieser Schlüssel für jedes Kommunikationsmodul I, II 7, 9 spezifisch ist, wird die Datenübertragung vom Kommunikationsmodul I 7 zum Kommunikationsmodul II 9 mit dem Schlüssel K_{Komm} I → II 23a und in umgekehrter Richtung mit dem Schlüssel K_{Komm} II → I 23b verschlüsselt. Die Entschlüsselung der verschlüsselten Daten erfolgt mit ebenfalls für jedes Kommunikationsmodul I, II 7 spezifischen Schlüsseln, die bei der erstmaligen Generierung der Verbindung zusammen mit den spezifischen Schlüsseln K_{Komm} 23 in Schlüsselpaaren derart in den Kommunikationsmodulen I, II 7, 9 abgelegt sind, daß Dritte sie nicht auslesen können.

In einem vierten Schritt wird die PIN über das Kommunikationsmoduls I 7 mit dem Schlüssel K_{Komm} I → II 23a verschlüsselt, über den sicheren Kanal 8 übertragen, über das Kommunikationsmodul II 9 entschlüsselt, dem zentralen Rechenwerk 10 in der geschützten Umgebung 12 übergeben.

In einem fünften Schritt wird in dem zentralen Rechenwerk 10 mittels des im zentralen Speicher 11 hinterlegten Schlüssel K_{PS} 16 und optional weiteren Daten die vom Benutzer eingegebene PIN verschlüsselt, wodurch die VPIN (verschlüsselte PIN) generiert wird.

Ihre Abbildung entspricht nun der Art, daß sie mit der auf der Chipkarte 1 abgespeicherten kartenindividuellen verschlüsselten EPIN 13 direkt verglichen werden kann.

In einem sechsten Schritt wird die VPIN in dem zentralen Rechenwerk 10 mittels des im zentralen Speicher 11 hinterlegten Schlüssel KGK_{PIN} 17 in eine spezielle Abbildung VVPIN (verschlüsselte verschlüsselte PIN) für den Transfer in die Chipkarte 1 umgeschlüsselt. Mittels der K_{PIN} 14 ist nur die spezifische Chipkarte 1 in der Lage, diese VVPIN zu VPIN zu entschlüsseln und diese mit der EPIN 13 zu vergleichen. In einem sechsten Schritt wird die VVPIN mittels des Kommunikationsmoduls II 9 mit dem Schlüssel K_{Komm} II → I 23b verschlüsselt, in dem sichern Kanal 8 übertragen, im Kommunikationsmodul I 7 entschlüsselt und der Chipkarte 1 übertragen.

In einem siebten Schritt wird die VVPIN mittels des Mikrocontrollers 2 im integrierten Rechenwerk 3 mittels des sich im integrierten Speicher 4 befindenden kartenindividuellen Schlüssels K_{PIN} 14 zu VPIN entschlüsselt und diese VPIN mit der im integrierten Speicher 4 befindlichen EPIN 13 verglichen.

In einem achten Schritt wird abhängig von dem Ergebnis dieses Vergleiches im integrierten Rechenwerk 3 des Mikrocontrollers 2 eine entsprechende Bearbeitungsroutine abgearbeitet. Im Fall der Identität ist der Benutzer als berechtigt identifiziert und der integrierte Rechner 3 kann unter Verwendung der Schlüssel K_{sonst} 15 und entsprechender Programmroutinen die Funktionen entsprechend des Verwendungszwecks tätigen.

Das erfindungsgemäße Verfahren eignet sich für alle sicherheitsrelevanten Anwendungen, bei denen eine sichere Identifikation von berechtigten Benutzern notwendig ist und diese Sicherheit innerhalb einer bestimmten Menge von Nutzern mittels identischer Schlüssel, die sich aus diesem Grund in einer besonders gesicherten Umgebung befinden müssen, und Chipkarten mit kartenindividuellen Schlüsseln realisiert wird. Ohne Beschränkung dieses allgemeinen Einsatzfeldes liegt der Schwerpunkt der Erfindung in der Nutzung innerhalb des bargeldlosen Zahlungsverkehrs. Die Chipkarte übernimmt in diesem Fall die Funktion einer Kreditkarte, einer kontobezogenen Börsenkarte, einer Händlerkarte, einer ec-Karte. In den verschiedenen Einsatzfällen werden entsprechende Schlüssel K_{sonst} 15 und Applikationsroutinen der Chipkarte 1 zur Ausführung der freigeschalteten Funktionsmodule, bsw. Geld von dem zugeordneten Konto abheben, verwendet. In diesem Anwendungsfall für den bargeldlosen Zahlungsverkehr entsprechen die speziellen Algorithmen und Schlüssel den zugeordneten standardisierten Schnittstellenspezifikationen, bsw. der Schnittstellenspezifikation für die ec-Karte mit Chip, Version 2.1.3 vom 27.10.95.

Bezugszeichenliste

1 Chipkarte
2 Mikrocontroller
3 integriertes Rechenwerk
4 integrierter Speicher
5 Chipkartenleser
6 Terminal
7 Kommunikationsmodul I
8 sicherer Kanal
9 Kommunikationsmodul II
10 zentrales Rechenwerk
11 zentraler Speicher
12 geschützte Umgebung

13 EPIN
14 K_{PIN}
15 K_{sonst}
16 K_{PS}
17 KGK_{PIN}
18 Kommunikationsmikrocontroller
19 interne CPU
20 interner Speicher
21 Selektionsmodul
22 Interface
23 K_{Komm}
23a K_{Komm} des Kommunikationsmoduls I
23b K_{Komm} des Kommunikationsmoduls I

Patentansprüche

1. Anordnung zur dezentralen Chipkartenidentifikation, wobei sich eine Chipkarte (1) mit einem Mikrocontroller (2), der ein integriertes Rechenwerk (3) und einen integrierten Speicher (4) beinhaltet, zur verwendungsgemäßen Benutzung in einem Chipkartenlesegerät befindet, die Chipkarte (1) die für ihren Betrieb notwendige Versorgungsspannung über das Chipkartenlesegerät bezieht, sich im integrierten Speicher (4) der Chipkarte (1) eine kartenindividuelle verschlüsselte EPIN (13) und ein ebenfalls kartenindividueller Schlüssel K_{PIN} (14) sowie weitere kartenindividuelle und in bestimmten Mengen einheitliche Schlüssel K_{sonst} (15) abgelegt, die mittels geeigneter Generierungsschlüssel an zentraler Stelle dynamisch generiert werden, **dadurch gekennzeichnet,**
daß ein spezieller Chipkartenleser (5) ein Terminal (6) und ein Kommunikationsmodul I (7) beinhaltet, welches über einen sicheren Kanal (8) mit einem Kommunikationsmodul II (9) in Wirkverbindung steht,
daß das Kommunikationsmodul 11(9) mit einem zentralen Rechenwerk (10) und einem zentralen Speicher (11) verbunden ist, welche sich in einer geschützten Umgebung (12) befinden, daß sich in dem zentralen Speicher (11) des zentralen Rechenwerks (10) innerhalb der geschützten Umgebung (12) ein für alle Chipkarten einheitlicher Schlüssel K_{PS} (16) und ein ebenfalls für alle Chipkarten einheitlicher Schlüssel KGK_{PIN} befindet,
daß die funktionell ähnlichen Kommunikationsmodule I, II (7), (9) jeweils aus einem Kommunikationsmikrocontroller (18), in dem eine interne CPU (19), ein interner Speicher (20), ein Selektionsmodul (21) und ein Interface (22) angeordnet sind, bestehen,
daß jedes Kommunikationsmodul I, II (7), (9) mittels des Selektionsmoduls (21) eindeutig identifizierbar ist, wobei mittels jeweils an autorisierter Stelle speziell generierten Schlüssel K_{Komm} (23), die durch Dritte nicht auslesbar sind, mittels Verschlüsselung der sichere Kanal (8) zwischen je zwei derartigen Kommunikationsmodule I, II (7), (9) aufgebaut werden, wobei das Interface (22) eine Schnittstelleneinheit zu einer geeigneten Zugangsstelle eines Datennetzes bezeichnet.

2. Verfahren zur dezentralen Chipkartenidentifikation, dadurch gekennzeichnet, daß für die dezentrale Chipkartenidentifikation im ersten Schritt der Benutzer durch die Inbetriebnahme des Chipkartenlesers (5) und durch das Einführen der Chipkarte (1) in den Chipkartenleser (5) die einzelnen verwendeten Module initialisiert, wobei in allen aktiven Mikrocontrollern die entsprechenden Grundinitialisierungsroutinen abgearbeitet werden,
im zweiten Schritt
der Benutzer zur Bezeichnung seiner Zugriffsberechtigung für die durch die Chipkarte (1) sicherheitsgemäß geschützte Anwendung über das Terminal (6) seine PIN eingibt und die korrekte Eingabe bestätigt,
im dritten Schritt
das Kommunikationsmodul I (7) des Chipkartenlesers (5) einen sicheren Kanal (8) mit dem Kommunikationsmodul II (9) des zentralen Rechenwerkes (10) innerhalb der geschützten Umgebung (12) aufbaut, wobei dies durch Verschlüsselung der zu übermittelnden Daten mit Hilfe des Schlüssels K_{Komm} (23) geschieht, wobei dieser Schlüssel für jedes Kommunikationsmodul I, II (7), (9) spezifisch ist, wobei die Entschlüsselung der verschlüsselten Daten mit ebenfalls für jedes Kommunikationsmodul I, II (7) spezifischen Schlüsseln erfolgt, die bei der erstmaligen Generierung der Verbindung zusammen mit den spezifischen Schlüsseln K_{Komm} (23) in Schlüsselpaaren auslesungssicher in den Kommunikationsmodulen I, II (7), (9) abgelegt sind,
im vierten Schritt
die PIN über das Kommunikationsmoduls I (7) mit dem Schlüssel K_{Komm} I → II (23a) verschlüsselt, über den sicheren Kanal (8) übertragen, über das Kommunikationsmodul II (9) entschlüsselt und dem zentralen Rechenwerk (10) in der geschützten Umgebung (12) übergeben wird,
im fünften Schritt
in dem zentralen Rechenwerk (10) mittels des im zentralen Speicher (11) hinterlegten Schlüssel K_{PS} (16) und optional weiteren Daten die vom Benutzer eingegebene PIN verschlüsselt und die VPIN generiert wird, wobei ihre Abbildung der Art entspricht, daß der Vergleich mit der auf der Chipkarte (1) abgespeicherten kartenindividuellen verschlüsselten EPIN (13) direkt gegeben ist,
im sechsten Schritt
die VPIN in dem zentralen Rechenwerk (10) mittels des im zentralen Speicher (11) hinterlegten Schlüssel KGK_{PIN} (17) in eine spezielle **Abb.** VVPIN für den Transfer in die Chipkarte (1) umgeschlüsselt wird, wobei mittels der K_{PIN} (14) nur die spezifische Chipkarte (1) in der Lage ist, diese VVPIN zu VPIN zu entschlüsseln und diese mit der EPIN (13) zu vergleichen,
im sechsten Schritt die VVPIN mittels des Kommunikationsmoduls II (9) mit dem Schlüssel K_{Komm} II → 1 (23b) verschlüsselt, in dem sichern Kanal (8) übertragen, im Kommunikationsmodul I (7) entschlüsselt und der Chipkarte (1) übertragen wird,
im siebten Schritt
die VVPIN mittels des Mikrocontrollers (2) im integrierten Rechenwerk (3) mittels des sich im integrierten Speicher (4) befindenden kartenindividuellen Schlüssels K_{PIN} (14) zu VPIN entschlüsselt und diese VPIN mit der im integrierten Speicher (4) befindlichen EPIN (13) verglichen wird,
im achten Schritt
abhängig von dem Ergebnis des Vergleiches aus Schritt 7 im integrierten Rechenwerk (3) des Mikrocontrollers (2) eine entsprechende Bearbeitungsroutine abgearbeitet wird, wobei im Fall der Identität der Benutzer als berechtigt identifiziert ist und der integrierte Rechner (3) unter Verwendung der Schlüssel K_{sonst} (15) und entsprechender Programmroutinen die Funktionen entsprechend des Verwendungszwecks tätigt.

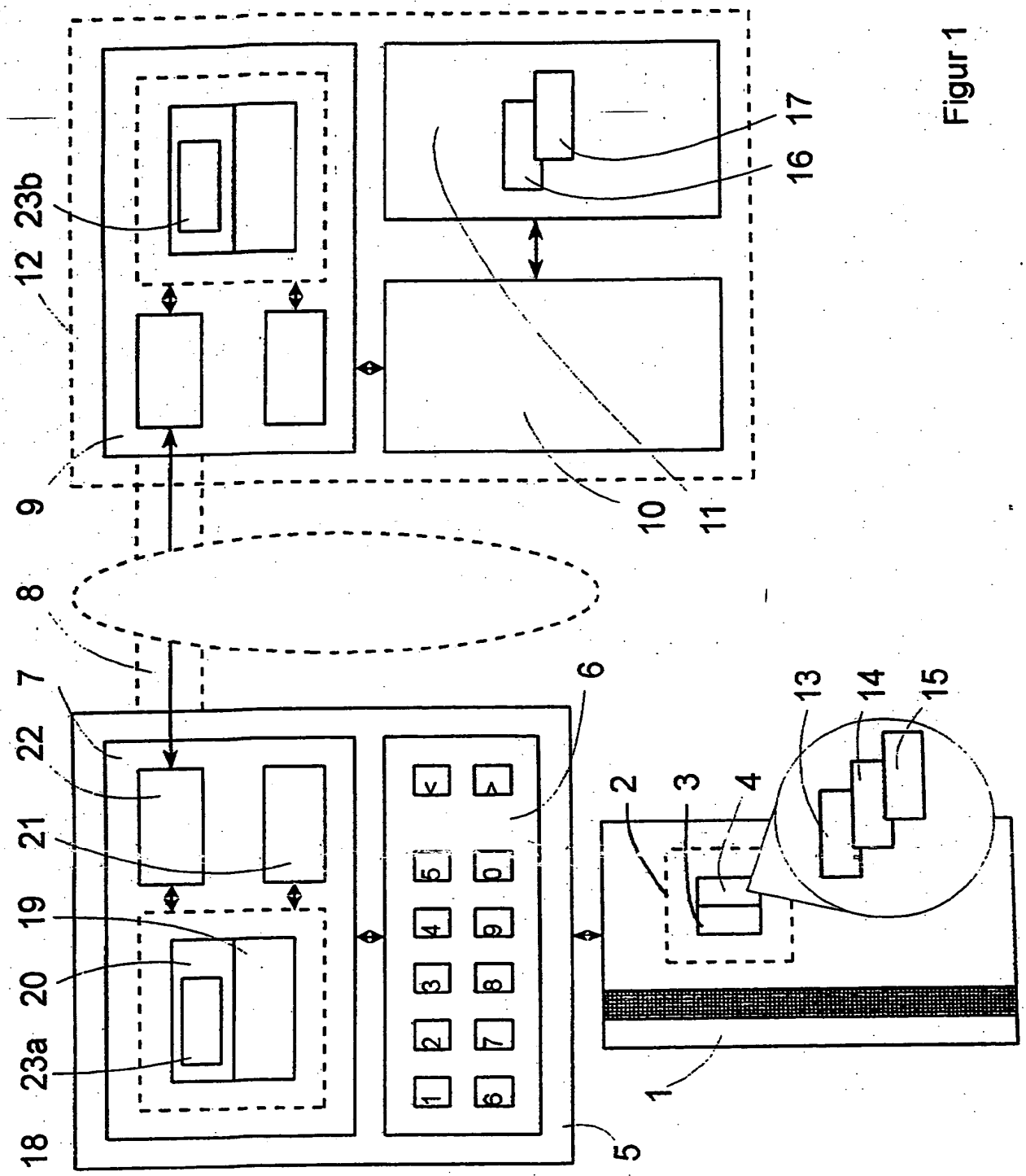
3. Verfahren zur dezentralen Chipkartenidentifikation nach Anspruch (1), dadurch gekennzeichnet, daß im Interesse eines hohen Datendurchsatzes das Kommuni-

kationsmodul II (9) für einen Parallelbetrieb ausgelegt ist.

4. Verfahren zur dezentralen Chipkartenidentifikation nach Anspruch (1), dadurch gekennzeichnet, daß im Anwendungsfall für den bargeldlosen Zahlungsverkehr die speziellen Algorithmen und Schlüssel den zugeordneten standardisierten Schnittstellenspezifikationen entsprechen.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 197 05 620 A1
Int. Cl.[6]: G 07 C 9/00
Offenlegungstag: 3. September 1998



Figur 1